Abstract

A security key distribution and authentication protocol in AAA for Mobile IP has been described. In order to guarantee the secure protocol, messages between the MN, FA, AAAF, AAAH, and HA are encrypted and signed using public/private keys. IPSEC or PKI infrastructure is not required to support the AAA secure key distribution. This protocol enhances the security, flexible, scalability of AAA, and aids in protecting the Diffie-Hellman algorithm from man-in-the-middle attacks. Through this protocol, it is easy to set up a secure registration path in AAA for Mobile IP. This secure registration path provides a secretive and secure key distribution function for AAA.

23552
PATENT TRADEMARK OFFICE

P03-0353-US1